CLAIMS

What is claimed is:

1. A method of operating a first security module, the method comprising the acts of:

detecting a second security module;

determining whether a key associated with the second security module is available to the first security module; and

obtaining the key associated with the second security module if the key associated with the second security module is not available to the first security module.

2. The method set forth in claim 1, comprising the act of configuring the first security module to be a trusted platform module ("TPM").

3. The method set forth in claim 1, comprising the act of requesting the key from the second security module.

4. The method set forth in claim 1, comprising the act of sending a public key from the first security module to the second security module if the key associated with the second security module is not available to the first security module.

5. The method set forth in claim 1, comprising the act of sending a public key along with validation information from the first security module to the second security module if the key associated with the second security module is not available to the first security module.

6. The method set forth in claim 1, comprising the act of storing the key in a memory associated with the first security module.

7. The method set forth in claim 1, comprising the act of defining the key to be a private key.

8. A security module, comprising:

a detector that is adapted to detect another security module and determine whether one of a plurality of keys is associated with the other security module; and

a device that obtains at least one key associated with the other security module if the one of the plurality of keys is not associated with the other security module.

9. The security module set forth in claim 8, wherein the security module comprises a trusted platform module ("TPM").

10. The security module set forth in claim 8, wherein the security module is adapted to request the at least one key from the other security module.

11. The security module set forth in claim 8, wherein the security module is adapted to send a public key to the other security module if the at least one key is not available to the security module.

12. The security module set forth in claim 8, wherein the security module is adapted to send a public key along with validation information to the other security module if the at least one key is not available to the security module.

13. The security module set forth in claim 8, wherein the at least one key is a private key.

14. A security module, comprising:

means for detecting another security module;

means for determining whether a key associated with the other security module is available to the security module; and

means for obtaining the key associated with the other security module if the key associated with the other security module is not available to the security module.

15. The security module set forth in claim 14, wherein the security module comprises a trusted platform module ("TPM").

16. The security module set forth in claim 14, wherein the security module is adapted to request the key from the other security module.

17. The security module set forth in claim 14, wherein the security module is adapted to send a public key to the other security module if the key associated with the other security module is not available to the security module.

18. The security module set forth in claim 14, wherein the security module is adapted to send a public key along with validation information to the other security module if the key associated with the other security module is not available to the security module.

19. The security module set forth in claim 14, wherein the security module is adapted to store the key in a memory associated with the security module.

20. The security module set forth in claim 14, wherein the key comprises a private key.

21. A computer system comprising:

a processor for executing program instructions;

a storage device for storing program instructions to be delivered to the processor;

at least one peripheral device that is controlled by the processor; and

a first security module associated with the at least one peripheral device, the first security module comprising:

a detector that is adapted to detect a second security module and determine whether one of a plurality of keys is associated with the second security module; and

a device that obtains at least one key associated with the second security module if the one of the plurality of keys is not associated with the second security module.

22. The computer system set forth in claim 21, wherein the first security module comprises a trusted platform module ("TPM").

23. The computer system set forth in claim 21, wherein the first security module is adapted to request the at least one key from the second security module.

24. The computer system set forth in claim 21, wherein the first security module is adapted to send a public key to the second security module if the at least one key is not available to the first security module.

25. The computer system set forth in claim 21, wherein the first security module is adapted to send a public key along with validation information to the second security module if the at least one key is not available to the first security module.

26. The computer system set forth in claim 21, wherein the at least one key is a private key.

27. A method of unsealing information from a plurality of security modules, the method comprising the acts of:

detaching an identifier from sealed information for one of the plurality of security modules;

decrypting the sealed information with a key that is associated with another of the plurality of security modules;

calculating a hash of the decrypted sealed information; and

comparing the calculated hash to the identifier to determine if the key was used to encrypt the sealed information.

28. The method set forth in claim 27, wherein the plurality of security modules comprise trusted platform modules ("TPMs").

29. The method set forth in claim 27, comprising the act of returning a decrypt key found message if the key is the key used to encrypt the sealed information.

30. The method set forth in claim 27, comprising the act of returning a decrypt key not found message if the key is not the key used to encrypt the sealed information.

31. A computer network, comprising:

a plurality of computer systems;

a network infrastructure that connects the plurality of computer systems together;

at least one of the plurality of computer systems comprising:

a first security module being configured to:

detect a second security module;

determine whether a key associated with the second security module is available to the first security module; and

obtain the key associated with the second security module if the key associated with the second security module is not available to the first security module.

32. The computer network, as set forth in claim 31, wherein the first security modules comprises a trusted platform module ("TPM").